said first correspondent having a private key and a public key derived therefrom, said method comprising the steps of:

a) said second correspondent obtaining said public key of said first correspondent;

b) said second correspondent sending a short-lived public key and said second correspondent's identity to said first correspondent;

c) said first correspondent combining its private key with said short-lived public key and generating a pair of secret keys therefrom;

d) said first correspondent using a first of said pair of secret keys to compute a first MAC on its identity, said second correspondent's identity, a random challenge, and said short-lived public key;

e) said first correspondent sending its identity, said random challenge, and said first MAC to said second correspondent, thereby requesting registration;

f) said second correspondent using said short-lived private key and said first correspondent's public key to generate said pair of secret keys;

g) said second correspondent verifying said first MAC using said first of said pair of secret keys;

h) said second correspondent using said first of said pair of secret keys to compute a second MAC on its identity, said first correspondent's identity, said random challenge, and said short-lived public key;

i) said second correspondent sending said second MAC to said first correspondent, thereby registering said first correspondent;

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

j) said first correspondent verifying said second MAC using said first of said pair of secret keys;

k) said correspondents each computing a pair of session keys from a second of said pair of secret keys, said short-lived public key, and said random challenge; and

l) said correspondents using at least one of said session keys in a secure communication.

A2

8. (New) A method according to claim 7, wherein said first correspondent is a mobile station and said second correspondent is a base station.

9. (New) A method according to claim 8, wherein said secure communication is a call originated by said mobile station.

10. (New) A method according to claim 8, wherein said secure communication is a call terminating at said mobile station.

11. (New) A method according to claim 8, wherein said secure communication is data exchange between said stations.

12. (New) A method according to claim 11, wherein said data exchange is used for internet browsing.

13. (New) A method according to claim 11, wherein said data exchange is used for financial transactions.

14. (New) A method according to claim 7, wherein said second correspondent obtains said public key from a service provider of said first correspondent.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

15. (New) A method according to claim 14, wherein said service provider obtains said public key by a manual exchange at a distributor outlet.

16. (New) A method according to claim 15, wherein said public key is transmitted to said service provider using a dial-up connection.

17. (New) A method according to claim 14, wherein said service provider obtains said public key by an exchange at manufacture time.

18. (New) A method according to claim 17, wherein said exchange comprises the steps of a manufacturer retrieving said public key, and transmitting said public key to said service provider.

19. (New) A method according to claim 14, wherein said service provider obtains said public key by an over-the-air exchange.

20. (New) A method according to claim 19, wherein said over-the-air exchange is secured using a password established between a user of said mobile station and said service provider.

21. (New) A method according to claim 19, wherein said over-the-air-exchange is secured using a password embedded in said mobile station at manufacture time.

22. (New) A method according to claim 7, wherein said second correspondent is a service provider of said first correspondent.

23. (New) A method according to claim 7, wherein the two MACs computed in step (e) each incorporate a value, said values being distinct from each other.

24. (New) A method according to claim 8, wherein the value used in said mobile station MAC is 2 and said base station MAC is 3.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

25. (New) A method according to claim 7, wherein said private keys, said public keys, and said MACs are computed using elliptic curve cryptography.

26. (New) A method according to claim 25, wherein said first correspondent is a mobile station and said second correspondent is a base station and said elliptic curve having a cofactor t, said short-lived public key is bP, said mobile station private key is m, and said pair of secret keys is generated from a shared secret tmbP.

27. (New) A base station for use in a communication system having at least one mobile station, each of said mobile stations having a secret key pair comprising a secret private key and a secret public key derived from said private key, access to said secret public key being restricted to a secure environment including said base station, said base station initiating communications with a respective one of said mobile stations by generating an ephemeral private key, obtaining therefrom a corresponding ephemeral public key, and forwarding said ephemeral public key to said mobile station, said base station computing a shared secret to be shared with said one of said mobile stations from said ephemeral key pair and said secret key pair to permit authentication of said stations to one another.

28. (New) A base station according to claim 27, wherein said base station obtains access to said secret public key from a service provider.

29. (New) A base station according to claim 27, wherein said base station is a service provider of said mobile station.

30. (New) A base station according to claim 29, wherein said base station obtains said public key by a manual exchange at a distributor outlet.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

31. (New) A base station according to claim 29, wherein said base station receives said public key using a dial-up connection.

32. (New) A base station according to claim 29, wherein said base station obtains said public key by an exchange at manufacture time.

33. (New) A base station according to claim 32, wherein said exchange comprises the manufacturer retrieving said public key, and transmitting said public key to said base station.

34. (New) A base station according to claim 32, wherein said base station obtains said public key by an over-the-air exchange.

35. (New) A base station according to claim 34, wherein said over-the-air exchange is secured using a password established between a user of said mobile station and said base station.

36. (New) A base station according to claim 34, wherein said over-the-air exchange is secured using a password embedded in said mobile station at manufacture time.

37. (New) A base station according to claim 27, wherein said secret key pair, said ephemeral key pair, and said authentication use elliptic curve cryptography.

38. (New) A method of establishing communications between a base station and a mobile station, wherein said mobile station has a secret key pair comprising a secret private key and a secret public key derived from said secret key, said method comprising the base station performing the steps of:

a) accessing said secret public key of said mobile station;

b) generating an ephemeral secret key;

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

c) obtaining from said ephemeral secret key a corresponding ephemeral public key;

d) forwarding said ephemeral public key bP to said mobile station; and

e) computing a shared secret from said ephemeral key pair and said secret key pair to permit authentication of said stations to one another.

39. (New) A method according to claim 38, wherein said base station accesses said secret public key by receiving said public key from a service provider;

40. (New) A method according to claim 38, wherein said base station is a service provider of said mobile station.

41. (New) A method according to claim 39, wherein said base station obtains said public key by a manual exchange at a distributor outlet.

42. (New) A method according to claim 39, wherein said base station receives said public key using a dial-up connection.

43. (New) A method according to claim 39, wherein said base station obtains said public key by an exchange of manufacture time.

44. (New) A method according to claim 42, wherein said exchange comprises the manufacturer retrieving said public key, and transmitting said public key to said base station.

45. (New) A method according to claim 42, wherein said base station obtains said public key by an over-the-air exchange.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

46. (New) A method according to claim 44, wherein said over-the-air exchange is secured using a password established between a user of said mobile station and said base station.

47. (New) A method according to claim 44, wherein said over-the-air-exchange is secured using a password embedded in said mobile station at manufacture time.

48. (New) A method for authenticating a first correspondent and a second correspondent in a communication system, wherein the first correspondent has a private key and a public key pair, said method comprising the steps of:

A2 Concl.

a) said second correspondent transmitting a short term public key along with an identifier to said first correspondent;

b) said first correspondent combining its private key with the second correspondent's short term public key and generating a pair of shared secret keys;

c) the correspondents using the first of said pair of shared secret keys for mutual authentication between said first and second correspondent;

d) the correspondents using the second shared secret key of said pair of shared secret keys for establishing a secret session key;

e) the correspondents using said secret key to provide confidentiality for authenticated communications in the communication system; said mutual authentication characterized in that the first correspondent authenticates itself to the second correspondent using its private key, and the second correspondent authenticates itself to the first correspondent using the fist correspondent's public key obtaining by said second correspondent from a trusted correspondent.

LAW OFFICES
FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000